IN THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the present application:

1. (Previously presented) A method of attempting to provide virus protection including the steps of:

receiving at a first location a request from a user for an object;

processing said request at a second location, wherein said step of processing includes scanning said object for viruses using a combination of vendors' products;

responding to said request, wherein said step of responding includes delivery of a response to said user.

2. (Original) The method of claim 1, wherein said request is in an electronic form.

3. (Currently amended) The method of claim 1, wherein said object is a file stored in a filer.

4. (Previously presented) The method of claim 3, wherein said step of processing said request further includes the steps of:

creating an access path from said filer to a processing cluster;

processing said file in said processing cluster; and

generating a report responsive to said processing of said file in said processing cluster.

5. (Original) The method of claim 4, wherein said step of creating an access path includes sending the ID and path of said file from said filer to said processing cluster.

6. (Original) The method of claim 5, wherein said step of sending is accomplished using non-uniform memory access.

7. (Original) The method of claim 5, wherein said step of sending is accomplished using a communications network.

8. (Original) The method of claim 5, wherein said step of sending is accomplished using a direct connection.

9. (Original) The method of claim 4, wherein said step of processing of said file is performed by said processing cluster in a round robin fashion for subsequent files received.

10. (Original) The method of claim 4, wherein said step of processing of said file is accomplished in parts by more than one device in said processing cluster.

11. (Previously presented) The method of claim 4, wherein all files stored on said filer are encrypted in a logical continuous manner.

12. (Previously presented) The method of claim 4, wherein said report contains a set of status data relating to said processing of said file.

13. (Original) The method of claim 12, wherein said status data includes at least one data element identifying the presence or non-presence of a virus in said file.

14. (Original) The method of claim 13, wherein said report is transferred to said filer.

15. (Original) The method of claim 14, wherein said report is stored in a first database.

16-17. (Canceled).

18. (Currently amended) The method of claim 3, wherein said ~~delivery of a~~ response is said file.

19. (Previously presented) The method of claim 3, wherein said delivery of a response includes notification to said user that said file is unavailable.

20. (Previously presented) The method of claim 4, wherein said step of responding to said request includes sending said user a copy of said report.

21. (Previously presented) An apparatus for attempting to provide virus protection including:

means for receiving at a first location a request from a user for an object;

means for processing said request at a second location, wherein said means for processing includes means for scanning said object for viruses using a combination of vendors' products;

means for responding to said request, wherein said means for responding includes delivery of a response to said user.

22. (Currently amended) The apparatus of claim 21, wherein said object is a file stored in a filer.

23. (Previously presented) The apparatus of claim 22, wherein said means for processing said request further includes:

means for creating an access path from said filer to a processing cluster;

means for processing said file in said processing cluster; and

means for generating a report responsive to said processing of said file in said processing cluster.

24. (Original) The apparatus of claim 23, wherein said means for creating an access path includes means for sending the ID and path of said file from said filer to said processing cluster.

25. (Previously presented) The apparatus of claim 24, wherein said sending is accomplished using non-uniform memory access.

26. (Previously presented) The apparatus of claim 24, wherein said sending is accomplished using a communications network.

27. (Previously presented) The apparatus of claim 24, wherein said sending is accomplished using a direct connection.

28. (Previously presented) The apparatus of claim 23, wherein said processing of said file is performed by said processing cluster in a round robin fashion for subsequent files received.

29. (Previously presented) The apparatus of claim 23, wherein said processing of said file is performed on atomic units of said file by more than one device in said processing cluster.

30. (Previously presented) The apparatus of claim 23, wherein all files stored on said filer are encrypted in a logical continuous manner.

31. (Previously presented) The apparatus of claim 23, wherein said report contains a set of status data relating to said processing of said file.

32. (Original) The apparatus of claim 31, wherein said status data includes at least one data element identifying the presence or non-presence of a virus in said file.

33. (Original) The apparatus of claim 31, wherein said report is transferred to said filer.

34. (Original) The apparatus of claim 33, wherein said report is stored in a first database.

35-36. (Canceled).

37. (Previously presented) The apparatus of claim 22, wherein said delivery of a response is delivery of said file.

38. (Previously presented) The apparatus of claim 22, wherein said delivery of a response includes delivery of notification to said user that said file is unavailable.

39. (Previously presented) The apparatus of claim 23, wherein said responding to said request includes sending said user some portion of said report.

40. (Previously presented) A method of attempting to provide virus protection in a client-server environment, comprising the steps of:

receiving a request at a server for a file;

sending, from the server, an identifier for the file to a cluster of scanning devices that scan the file for viruses using a combination of vendors' products;

receiving, at the server, an indication from the scanning devices as to whether or not the file is safe to send from the server; and

responding to the request by sending the file if the indication is that the file is safe to send.

41. (Previously presented) A method as in claim 40, wherein the scanning devices indicate that the file is safe to send if the scanning devices determine that the file is not infected with any viruses.

42. (Previously Presented) A method as in claim 40, wherein the request is received from and the file is sent to a client device.

43. (Previously Presented) A method as in claim 40, wherein the server is a web server.

44. (Canceled).

45. (Currently amended) A method as in claim [[44]] 40, wherein the cluster of devices is a cluster of interconnected personal computers.

46-56. (Canceled).

57. (Previously presented) A server that attempts to provide virus protection in a client-server environment, comprising:

a communication link to client devices;

mass storage for files; and

a processor that executes instructions in order to send requested files to the client devices, the instructions also including instructions (a) to receive a request for a file, (b) to send an identifier for the file to a cluster of scanning devices that scan the file for viruses using a combination of vendors' products, and (c) to respond to the request by sending the file.

58. (Canceled).

59. (Previously Presented) A server as in claim 57, wherein the request is received from and the file is sent to a client device.

60. (Previously Presented) A server as in claim 57, wherein the server is a web server.

61. (Canceled).

62. (Currently Amended) A server as in claim 57, wherein the cluster of devices is a cluster of interconnected personal computers.

63-73. (Canceled).

74. (Currently amended) Storage containing information including instructions, the instructions executable by a processor to attempt to provide virus protection in a client-server environment, the instructions ~~comprising~~ to configure the processor to perform the steps of:

receiving a request at a server for a file;

sending, from the server, an identifier for the file to a cluster of scanning devices that scan the file for viruses using a combination of vendors' products;

receiving, at the server, an indication from the scanning devices as to whether or not the file is safe to send from the server; and

responding to the request by sending the file if the indication is that the file is safe to send;

wherein communication between the server and the cluster of scanning devices is performed using non-uniform memory access.

75. (Previously presented) Storage as in claim 74, wherein the scanning devices indicate that the file is safe to send if the scanning devices determine that the file is not infected with any viruses.

76. (Previously Presented) Storage as in claim 74, wherein the request is received from and the file is sent to a client device.

77. (Previously Presented) Storage as in claim 74, wherein the server is a web server.

78. (Canceled).

79. (Previously presented) Storage as in claim 74, wherein the cluster of devices is a cluster of interconnected personal computers.

80-90. (Canceled).

91. (Currently amended) Storage containing information including instructions, the instructions executable by a processor to provide virus protection, the instructions ~~comprising~~ to configure the processor to perform the steps of:

receiving at a first location a request from a user for an object;

processing said request at a second location, wherein said step of processing includes scanning said object for viruses using a combination of vendors' products;

responding to said request, wherein said step of responding includes delivery of a response to said user.

92. (New) A method comprising:

receiving a request at a web server for a file from a client;

sending, from the web server, an identifier for the file to a cluster of interconnected personal computers that scan the file simultaneously for viruses using a combination of vendors'

products, wherein communication between the web server and the cluster of interconnected personal computers is performed using non-uniform memory access;

receiving, at the web server, an indication from the cluster of interconnected computers as to whether or not the file is infected with a virus; and

responding to the request by sending the file to the client if the indication is that the file is not infected with a virus.

93. (New) A method of providing virus protection, comprising:

receiving at a first location a request for an object;

processing said request at a second location, wherein said step of processing includes scanning said object for virus using a combination of vendors' products; and

responding to said request, wherein said step of responding includes delivery of a response.